DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

IN REPLY REFER TO

OTS 730.3.A

October 22, 2002
02-OTS-061(R)

MEMORANDUM FOR REGIONAL DIRECTORS, DCAA
DIRECTOR, FIELD DETACHMENT, DCAA
HEADS OF PRINCIPAL STAFF ELEMENTS, HQ, DCAA

SUBJECT: Audit Management Guidance on Issuing Electronic Audit Reports and Preparing/Filing Supplemental/Revised Working Papers and Reports in APPS/iRIMS

This memorandum establishes guidance on:

- Issuing electronic audit reports (Section A)
- Issuing supplemental/revised reports with updated working papers (Section B)
- Issuing revised reports without updated working papers (Section C)
- Archiving audit working papers and reports, including iRIMS (Section D)
- Updating final report and signature page file naming conventions (Section E)
- Handling large audit files and reports (Section F)

A. Issuing Electronic Audit Reports

To the maximum extent possible, all written correspondence and audit reports should be transmitted electronically to requestors and customers via e-mail. DCAA e-mail to DoD components will be sent only through Defense Information Systems Agency (DISA) supported communications channels, ".mil" addresses. NASA Headquarters Office of Procurement has also authorized its NASA Centers (generally ".nasa.gov" addresses) to request and receive DCAA audit reports electronically. Procedures for electronic communications with other non-DoD customers should be determined on a case-by-case basis after consultation with the customer and your regional information technology (IT) staff. Transmission of "For Official Use Only" material using private and commercial service providers such as AOL or CompuServe is prohibited.

OTS 730.3.A
SUBJECT: Audit Management Guidance on Issuing Electronic Audit Reports and Preparing Supplemental/Revised Working Papers and Reports in APPS/iRIMS

Electronic files prepared using Microsoft Office products can be saved in a variety of formats and software versions. Thus, it is critical to communicate with customers to determine the version and brand of software they are using. Based on customer requirements, choose the appropriate format and version that provides the best opportunity for the customer's efficient use of the audit report and any accompanying files or attachments.

Due to the limitations in file size that can be accommodated by e-mail software and servers, large electronic files (over 500kb) should be compressed. Options for compressing include the use of self-extracting ".exe" files using software programs such as WinZip, which is the DCAA standard. Be aware, however, that due to security concerns some e-mail servers do not accept e-mails containing files with the ".exe" extension. Thus some attempts to send ".exe" files to the customer may be rejected.

One option is to rename the file name. Ensure that the recipient is aware that they will have to rename it with the ".exe" once they receive the document. Therefore, ensure you coordinate closely with your recipients prior to selecting your method of file compression. Before the document is sent electronically, it must be password protected using the "Password to Modify" option to restrict modifications and prevent accidental changes being made to the document after receipt. Your regional IT staff should be consulted if problems arise while attempting to activate this feature in your Microsoft Office software. Please note, however, that the modification protection does not prevent the addressee from opening, copying, and using it in any appropriate way in support of his or her mission. (Note that the requirement to store the report password in the audit file has been rescinded.)

Cover e-mail messages for audit reports should only include administrative-type information. Cover messages will provide information such as: (1) name of document attached, (2) software used to prepare the report; e.g. Microsoft Word XP, (3) comment that the audit report is classified "For Official Use Only", (4) comment regarding the use of password protection of the document to guard against modification, (5) instructions for opening the compressed file(s), and (6) if applicable, whether and why an electronic report is incomplete. An example cover message follows:

Attached is subject audit report [provide file name] which is prepared in [specify the specific version of Microsoft Word]. The attached report is For Official Use Only. While it is password protected from accidental changes, it can be opened as a "read only" document without using the password. However, information within the report can be copied to a new document for analysis purposes.

The report was compressed using [specify the software used and whether the file was saved as a self-extracting file or not]. To extract (decompress) the report [provide specific steps to the user on how to extract the file].

If you have difficulty opening the audit report document or have other questions, please contact [provide points of contact to the customer, including telephone number and e-mail address].

B. Issuing Supplemental Reports with Updated Working Papers

In most instances, supplemental reports require the updating or modification of audit working papers contained in the original audit file. When this occurs, the original file must be left intact. A complete copy of the original file should be made and updated to reflect the updated audit work and audit report as follows:

1. Make a copy of the .EXE file from the official file.
2. Restore the file into APPS using the "Import" function from the "Electronic Audit Packages" menu.
3. Keep all of the original working papers and update them as needed. There is no need to rename the working papers to show that they have been supplemented or revised. However, changed working papers should be re-dated showing the new completion date and supervisory review date. Also replace the auditor's and/or supervisor's initials if either has changed from the original working paper(s).
4. If any working papers become superceded, they should be moved into the "Superceded Working Papers" folder.
5. Add new working papers as needed.
6. Issue the supplemental report adding an "-S1" to the original report name. If additional supplemental reports are issued, increase the numeric indicator, e.g. -S2, -S3, etc. For example, a supplemental report might be named 01 DCAA Report 01101-2002A21000001-Final-S1.DOC
7. Create a new archive file which includes all working papers and supplemental or revised report into an .EXE file using the APPS functions "Electronic Audit Packages", "Admin Functions", "Save as Archive".
8. Name the new archive file using the following naming convention: RORG-Assignment No.-S1.EXE for supplemental reports incrementing the numeric indicator as explained above for subsequent supplemental or revised reports. For example, 01101-2002A21000001-S1.EXE.

C. Issuing Revised Reports without Updated Working Papers

In some instances, a revised report can be issued without a need to modify working papers. One example would be where a schedule was inadvertently omitted from the audit report but was readily available in the working papers. When a revised report is issued without changing working papers, you should:

1. Make a copy of the audit report from the official file.
2. Make the necessary corrections.
3. Issue the revised report by adding a "-R1" to the original report name.

4. The revised report will be archived using the instructions below. Because there are no new or revised working papers, only the revised report and the scanned signature page will be archived.

D. Archiving Audit Working Papers and Reports, including iRIMS

While the Agency is deploying iRIMS as its electronic archiving process, FAOs will need to store all audit files using the non-iRIMS (current) process. As FAOs begin using iRIMS, both methods shown below must be used until we verify that the iRIMS process has been completely deployed and that files are being archived reliably 100% of the time.

Non-iRIMS

1. The original official and backup CDs shall be left intact in the official file and backup storage container.
2. Two CDs will be made of the supplemental/revised files using the procedures in CAM 4-407d "Completed Working Paper Packages - Final Storage." The only change is that this second set of CDs will include the designator –S1 or –R1 in the file name immediately preceding the .EXE extension and the scanned signature page will be included. For example, the two supplemental files would be named 01101-2002A21000001-Final-S1.EXE for the official file and 01101-2002A21000001-Archive-S1.EXE for the backup. The scanned signature page should be named using the convention shown in paragraph 2c, below.

iRIMS

1. In accordance with iRIMS business rules (refer to MRD 02-CM-031(R) dated 8/15/02), a folder should be established for each assignment. All revised and supplemental working papers and reports will be stored in this folder.
2. For supplemental and revised reports, the following will be filed:
   a. If updated working papers have been prepared, the archive file (.EXE) created in step B8, above.
   b. The audit report file created in step B6 or C3, above.
   c. A scanned image of the audit report signature page. This will usually be a .TIF file. The naming convention for this page is to use the audit report file name as the prefix in the file name with a TIF suffix. For example, "01 DCAA Report 01101-2002A21000001-Final-sig-S1.tif" would be a typical supplemental audit report file name.

E. Revised Final Report and Signature Page File Naming Convention

The recent MRD 02-PAS-068(R), dated September 13, 2002, established a new naming convention for the signed version of the report file and the image file of the signature page of the report. The naming convention established by that MRD did not begin with the "01" index

number usually associated with the report in the working paper package. Without the "01" designator APPS does not display the report under the "Admin WPs" tab where it is usually located. The new enhanced APPS is expected to incorporate the ability to display the report correctly without the "01" designation; however, its expected implementation date is now set to begin in March 2003. Therefore, the naming convention for the final audit report and the scanned signature page files are revised as follows until the adoption of the enhanced APPS, at which time the "01" may be dropped:

Final Report Electronic File:

Once an audit report is signed, the file used to print that report should be renamed to uniquely identify that file as the official report. Currently the APPS can be used to create a copy of the draft audit report for final processing. The copy created by APPS is named "01 - Final Audit Report.doc." This file is processed to accept/reject tracked changes, remove cross-references and comments, remove hyperlinks to other documents, unlink document variables, and make final formatting changes before the report is printed out and signed. Once an audit report is signed, the electronic document should immediately be modified to indicate who signed it and it should be password protected. The electronic file should then be renamed according to the convention "01 DCAA Report [RORG-ASSIGNMENT NO.]-Final.doc" and changed to a read-only file. Only this file should be stored, transmitted, or otherwise used for official purposes.

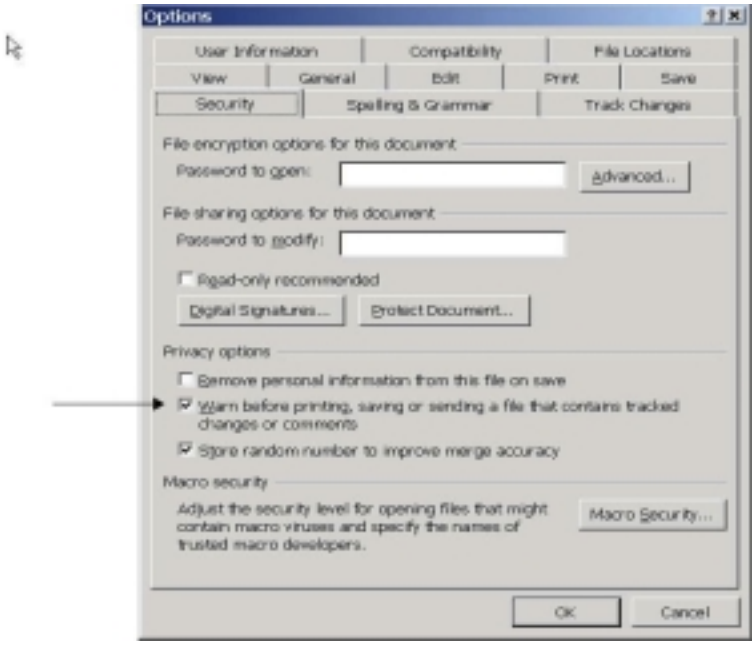
Signature Page Image File

The scanning of the signature page is required for all DCAA audit reports. We recommend that the report be signed using black ink because scanners do not always pick up blue ink. The Agency standard scanning instructions can be found on the Intranet at https://computersupport.dcaaintra.mil/scanner/ScannerProcedures.pdf. For audit packages, the scanned signature page should be named the same as the report (see above) with "–sig" added and an image file extension (i.e., 01 DCAA Report 01101-2002X10100389-Final-sig.tif). There is no requirement to make the .TIF file a part of the APPS generated executable file and it may be included separately on the CD containing the APPS generated executable file.

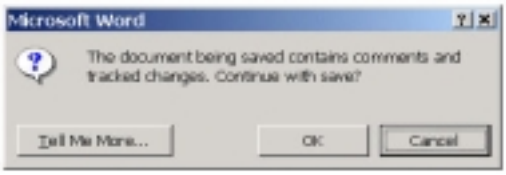
Ensuring the Removal of Comments and Track Changes

The reviewing toolbar in Microsoft Word XP now includes a **Display for Review** drop down menu box which includes four options (**Final, Final Showing Markup, Original and Original Showing Markup**). In **Final** view, track changes and reviewer's comments are hidden. To ensure all track changes have been permanently accepted or rejected, you must first turn off track changes and then select the reviewing toolbar **Display for Review** option of "**Final Showing Markup.**" For added assurance against issuing reports or correspondence with track changes still accessible by the recipient, we recommend that all auditors and administrative personnel who send correspondence or reports outside the FAO activate a built-in warning from the "**Tools**" drop down menu, then select "**Options**" then the "**Security**" tab and then checking

the box called "**Warn before printing, saving or sending a file that contains tracked changes or comments**" as shown below. (You may also refer to Western Region's Intranet site (Regional News, Focus on Quality, Quality Assurance Division Home Page, Quality Alert 2002-05.)



Before printing or saving, you will be warned if there are comments or unaccepted changes with the following message.



While the security tab infers that a warning will be displayed if the document is sent, this is true only in limited circumstances and you should not rely upon a warning being displayed from Outlook XP.

F. Handling Large Audit Files and Reports.

As we move to a more paperless process, we need to ensure that we do not create electronic files that become so large that they are difficult to store, e-mail or otherwise handle. When scanning or otherwise obtaining electronic files, we need to ensure that we are obtaining and retaining only necessary data and that we properly prepare audit reports and working papers.

1. **Unnecessary copies of contractor data**. Copies of detailed contractor data and documents (including detailed portions of the contractor's proposal or submission) should not be retained if the contractor is already required to maintain the data, documents, or proposal unless the data forms the basis of a significant finding. Generally auditors only need to reference contractor data and documents reviewed and may extract specific portions to which they take exception. This is current Agency policy as extracted from the CAM, below:

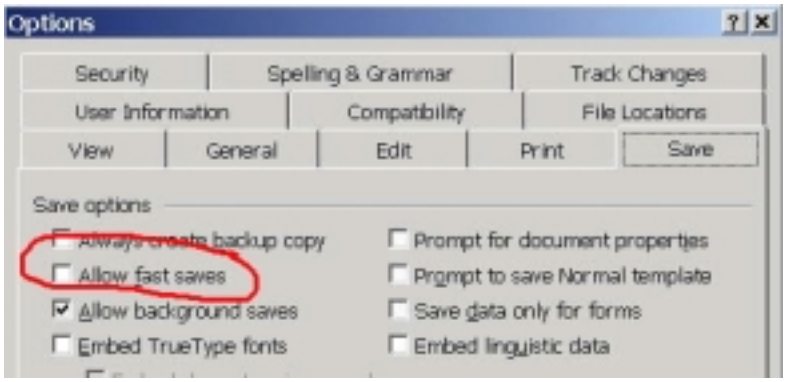
   4-406 Copies of Contractor Data in Working Papers
   a. When considering the extent of the contractor's data that should be copied and retained in the working paper files, use the following guidelines:
      (1) Keep copies of contractor financial records and documents to the minimum necessary to support the information obtained and the conclusions reached. Consider the continuing availability of source documents and contract data retention requirements when deciding whether to reference or reproduce contractor source documents.
      (2) Where a particularly sensitive or material audit conclusion hinges on key source documents and referencing would not provide sufficient evidence of the content, include copies in the working papers. This same consideration applies when the audit results can give rise to a government claim against the contractor such as an assertion of defective pricing or an allegation of CAS noncompliance. In these situations, the contractor data should be retained in the working paper files for consideration by the contracting officer in his/her decision making processes. More routine audit conclusions may be sufficiently documented by reference and extraction of pertinent information.
      (3) Recognize contractor concerns about reproducing copies of sensitive financial or other operating information. Instead of making copies, take notes or extracts if this will satisfy the government auditing standards and the needs of the contracting officer can be accomplished with a reasonable expenditure of audit effort.

2. **Inefficient file format**. When it is necessary to retain copies of contractor data or documents, it should be in an efficient format. Pages scanned in accordance with Agency guidance will usually be less than 100 kilobytes in file size; however, if the settings are incorrect a single page can take up several megabytes (e.g., when saved as a .BMP file rather than a .TIF file). A document saved in an .RTF format can be several times larger than the same document saved in a .DOC format. All overly large files should be reviewed to ensure they are in the most efficient format and do not contain unnecessary images or data.

3. **Unnecessary embedded data or images**. Significant amounts of data can be embedded or imported in a document or spreadsheet without realizing the significant impact on file size. Images may be pasted into a document as a .bmp file which can make the document very large, but it may not be easily identified because it is embedded in the document and

the auditor cannot see it is in the .bmp format. Similarly, Excel spreadsheets should not be embedded into audit reports although that process can be used in working papers. Instead, data should be pasted into the audit report as tables. When issuing audit reports, a good rule of thumb is that the file size should be about 50 to 100 kilobytes per page. If your report is significantly larger, it should be checked. Your regional RSA staff can provide assistance.

4. **"Fast Saves" should not be used**. In Microsoft Word, the user can elect to use fast saves; however, we strongly discourage that process. Fast saves do not remove deleted information from the file; instead it only removes it from sight. Where significant amounts of cutting and pasting are used, this can dramatically increase file size. To turn off fast saves, select Tools, Options and click on the Save tab. Make sure that the fast saves check box is not checked as shown below.



Questions or comments on this memorandum should be directed to Mr. David Roll, Chief, Technical Audit Services Division, at (703) 767-2295 or Dave.Roll@dcaa.mil.

/s/

Earl J. Newman
Assistant Director
Operations

DISTRIBUTION: C